PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-202895
(43)Date of publication of application : 19.07.2002

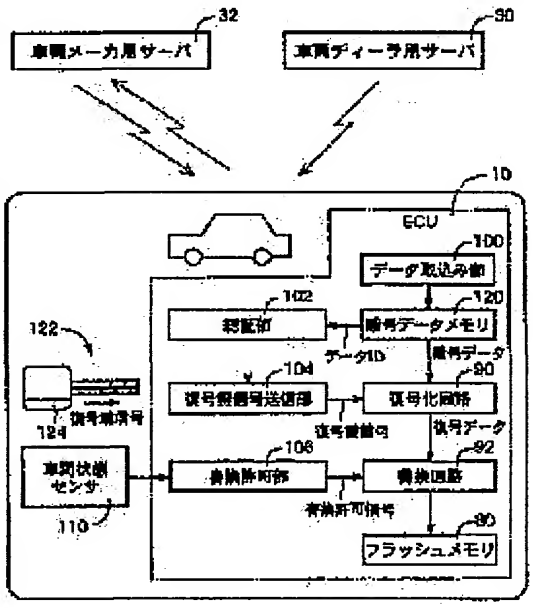
(51)Int.Cl. G06F 11/00
G05B 15/02
G06F 1/00

(21)Application number : 2000-400519
(22)Date of filing : 28.12.2000

(71)Applicant : TOYOTA CENTRAL RES & DEV LAB INC
(72)Inventor : NAKAJO NAOYA
WADA TAKASHI
KATO SATORU
MAEDA MITSUTOSHI
YONEMURA MASATOSHI
ITO HIROSHI

(54) DEVICE FOR UPDATING VEHICLE BASIC FUNCTION CONTROL PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To update the contents of a vehicle basic function control program without performing the overall or partial exchange of an onboard computer for executing a vehicle basic function control program.
SOLUTION: Cipher data necessary for updating a vehicle basic function control program are fetched by a data fetching part 100 by radio waves transmitted from a server 30 for a vehicle dealer. The contents of a vehicle basic function control program are updated in a flash memory 80 in which the vehicle basic function control program is stored by a decoding circuit 90 and a rewriting circuit 92 based on the fetched cipher data.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－202895
（P2002－202895A）
(43)公開日　平成14年７月19日(2002.7.19)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　11/00		Ｇ０５Ｂ　15/02	Ｐ	５Ｂ０７６
Ｇ０５Ｂ　15/02		Ｇ０６Ｆ　9/06	６３０Ａ	５Ｈ２１５
Ｇ０６Ｆ　1/00			６６０Ｆ	

審査請求　未請求　請求項の数10　ＯＬ　（全 10 頁）

(21)出願番号　特願2000－400519(P2000－400519)

(22)出願日　平成12年12月28日(2000.12.28)

(71)出願人　000003609
株式会社豊田中央研究所
愛知県愛知郡長久手町大字長湫字横道41番地の１

(72)発明者　中條　直也
愛知県愛知郡長久手町大字長湫字横道41番地の１　株式会社豊田中央研究所内

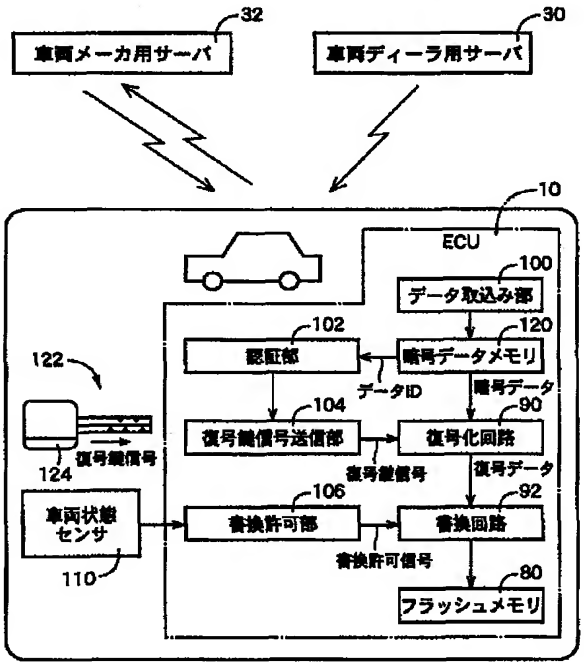
(72)発明者　和田　隆志
愛知県愛知郡長久手町大字長湫字横道41番地の１　株式会社豊田中央研究所内

(74)代理人　100107674
弁理士　来栖　和則

最終頁に続く

(54)【発明の名称】　車両基本機能制御プログラム更新装置

(57)【要約】
【課題】車両基本機能制御プログラムを実行する車載コンピュータの全体的または部分的な交換を伴わずにその車両基本機能制御プログラムの内容を更新することを可能にする。
【解決手段】車両ディーラ用サーバ３０から送信された電波により、車両基本機能制御プログラムの更新を行うために必要な暗号データを、データ取込み部１００において取り込む。その取り込まれた暗号データに基づき、復号化回路９０および書換回路９２により、車両基本機能制御プログラムを記憶したフラッシュメモリ８０においてその車両基本機能制御プログラムの内容を更新する。



1

【特許請求の範囲】

【請求項１】　車両の基本機能を制御するためにその車両に搭載されたコンピュータにより実行される車両基本機能制御プログラムであってそのコンピュータのプログラムメモリに記憶されているものを更新するためにその車両に搭載された装置であって、

前記更新を行うために前記プログラムメモリに対して実行することが必要である処理の内容を定義する処理内容定義データを取り込むデータ取込み部と、

その取り込まれた処理内容定義データに基づき、前記処理を前記プログラムメモリに対して実行することにより、前記車両基本機能制御プログラムを更新するプログラム更新部とを含む車両基本機能制御プログラム更新装置。

【請求項２】　前記データ取込み部が、外部からオンラインで送信された前記処理内容定義データを受信するデータ受信部を含む請求項１に記載の車両基本機能制御プログラム更新装置。

【請求項３】　前記処理内容定義データが、可搬性を有する記録媒体に記録されたものであり、前記データ取込み部が、前記車両に搭載されたデータ読取り装置であって前記記録媒体が装填されてその記録媒体から前記処理内容定義データを読み取るものを含む請求項１に記載の車両基本機能制御プログラム更新装置。

【請求項４】　前記処理内容定義データが、前記処理の内容が暗号化された暗号データであり、前記プログラム更新部が、その暗号データが入力された場合に、その入力された暗号データを復号化する復号化部を含む請求項１ないし３のいずれかに記載の車両基本機能制御プログラム更新装置。

【請求項５】　さらに、前記車両が、前記取り込まれた処理内容定義データにより定義される処理が前記プログラムメモリに対して実行されることが予定された車両である予定プログラム更新対象車両ではない場合に、前記プログラム更新部による更新を禁止する第１更新禁止部を含む請求項１ないし４のいずれかに記載の車両基本機能制御プログラム更新装置。

【請求項６】　さらに、前記車両の実際のユーザがその車両の真の所有者でもその真の所有者により許可された者でもない場合に、前記プログラム更新部による更新を禁止する第２更新禁止部を含む請求項１ないし５のいずれかに記載の車両基本機能制御プログラム更新装置。

【請求項７】　前記プログラム更新部が、それが更新すべき前記車両基本機能制御プログラムを実行する前記コンピュータと同じコンピュータにより作動させられるものである請求項１ないし６のいずれかに記載の車両基本機能制御プログラム更新装置。

【請求項８】　さらに、前記コンピュータの負荷状態が設定状態を超えている場合に、前記プログラム更新部による更新を禁止する第３更新禁止部を含む請求項７に記

2

載の車両基本機能制御プログラム更新装置。

【請求項９】　前記第３更新禁止部が、前記車両が実質的に停止状態にはない場合に、前記コンピュータの負荷状態が設定状態を超えている場合であるとして、前記プログラム更新部による更新を禁止する更新禁止手段を含む請求項８に記載の車両基本機能制御プログラム更新装置。

【請求項１０】　さらに、前記車両が実質的に停止状態にはない場合に、前記プログラム更新部による更新を禁止する第４更新禁止部を含む請求項１ないし９のいずれかに記載の車両基本機能制御プログラム更新装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、車両の基本機能を制御するためにその車両に搭載されたコンピュータにより実行される車両基本機能制御プログラムを更新する技術に関するものである。

【０００２】

【従来の技術】コンピュータの性能の飛躍的向上を背景に、自動車、オートバイ等の車両の分野においては、それの基本機能、すなわち、「走る」、「曲がる」および「止まる」といった動作の性能を向上させるとともに、ユーザの多様なニーズに応えるべく、その基本機能をコンピュータにより電子制御する技術が広く採用されている。

【０００３】このような技術を採用した電子制御車両は、一般に、コンピュータが搭載されるとともに、その車両の基本機能を制御するためにそのコンピュータにより実行される車両基本機能制御プログラムが、そのコンピュータのプログラムメモリに記憶される。

【０００４】この種の電子制御車両においては、その車両基本機能制御プログラムをみだりに変更することは、その車両の基本機能が設計通りに実現されなくなってしまうことにつながるため、許されるべきではない。

【０００５】そのため、従来においては、この種の電子制御車両は、それのユーザはもちろん、その車両を取り扱う業者（製造業者、販売業者、修理業者等）ですら、その車両のコンピュータの全体的または部分的な交換なしで車両基本機能制御プログラムを書き換えることが基本的には不可能であるように設計されていた。

【０００６】

【発明が解決しようとする課題】車両の基本性能を向上させる等の目的のもと、例えば、その車両のメーカサイドが、その車両に既に搭載されている車両基本機能制御プログラムの内容を更新したいと要望する場合がある。

【０００７】しかし、従来の電子制御車両においては、前述の説明から明らかなように、その車両のコンピュータの全体または一部を交換しない限り、車両基本機能制御プログラムの内容を更新することが、そのコンピュータの構造上、禁止されていた。

【０００８】そのため、電子制御車両のユーザは、車両基本機能制御プログラムの内容を更新することが必要である場合には、わざわざ車両のディーラや修理工場、サービステーション等にその車両を持ち込んで、ある期間、その車両を預けておかなければならず、不便であった。

【０００９】

【課題を解決するための手段および発明の効果】それらの事情に鑑み、本発明は、コンピュータの全体的または部分的な交換を伴わずに車両基本機能制御プログラムの内容を更新することを可能にすることを課題としてなされたものであり、本発明によって下記各態様が得られる。各態様は、請求項と同様に、項に区分し、各項に番号を付し、必要に応じて他の項の番号を引用する形式で記載する。これは、本明細書に記載の技術的特徴のいくつかおよびそれらの組合せのいくつかの理解を容易にするためであり、本明細書に記載の技術的特徴やそれらの組合せが以下の態様に限定されると解釈されるべきではない。

【００１０】（１）　車両の基本機能を制御するためにその車両に搭載されたコンピュータにより実行される車両基本機能制御プログラムであってそのコンピュータのプログラムメモリに記憶されているものを更新するためにその車両に搭載された装置であって、前記更新を行うために前記プログラムメモリに対して実行することが必要である処理の内容を定義する処理内容定義データを取り込むデータ取込み部と、その取り込まれた処理内容定義データに基づき、前記処理を前記プログラムメモリに対して実行することにより、前記車両基本機能制御プログラムを更新するプログラム更新部とを含む車両基本機能制御プログラム更新装置［請求項１］。この装置においては、車両基本機能制御プログラムの更新を行うためにプログラムメモリに対して実行することが必要である処理の内容を定義する処理内容定義データがデータ取込み部において取り込まれ、その取り込まれた処理内容定義データに基づき、プログラム更新部により、上記処理がプログラムメモリに対して実行され、それにより、車両基本機能制御プログラムが更新される。したがって、この装置によれば、コンピュータのうちの少なくともプログラムメモリを含む部分を交換することなく、そのプログラムメモリにおいて車両基本機能制御プログラムの内容を更新可能となる。よって、この装置によれば、車両のユーザは、車両基本機能制御プログラムの更新のためにわざわざ特定の場所に出向くことが不要となり、その結果、この装置によれば、車両基本機能制御プログラムの更新が容易になる。本項において「プログラム更新部」は、車両基本機能制御プログラムを実行するためのコンピュータまたはそれとは別のコンピュータの一部として構成したり、それらコンピュータの一部と、電子回路との組み合わせとして構成することが可能である。後者の態様においては、例えば、後に実施形態において説明するように、電子回路を、それらコンピュータの一部からの指令信号に応答して起動するように設計することが可能である。また、本項において「処理内容定義データ」の一例は、現在の車両基本機能制御プログラムの全部または一部が更新されるべき内容を有するプログラムを含み、かつ、そのプログラムでその現在の車両基本機能制御プログラムの全部または一部を書き換えることを、その車両基本機能制御プログラムを実行するためのコンピュータまたはそれとは別のコンピュータに指令することを定義するデータとすることができる。また、「処理内容定義データ」の別の例は、現在の車両基本機能制御プログラムの一部を無効にし、または削除することを、その車両基本機能制御プログラムを実行するためのコンピュータまたはそれとは別のコンピュータに指令することを定義するデータとすることができる。また、本項において「更新」という用語は、例えば、追加、変更、書換、削除等の少なくとも１つを含むように解釈することが可能である。

（２）　前記データ取込み部が、外部からオンラインで送信された前記処理内容定義データを受信するデータ受信部を含む（１）項に記載の車両基本機能制御プログラム更新装置［請求項２］。この装置においては、車両基本機能制御プログラムの更新が、外部からオンラインで送信された処理内容定義データに基づいて行われる。したがって、この装置は、車両のユーザが、車両基本機能制御プログラムの更新のために特定の物を使用して特定の作業を行うことが不要である態様で実施することが可能である。本項において「オンライン」でのデータ送信は、無線の通信回線（電波、光）を利用して行うことや、有線の通信回線を利用して行うことが可能である。

（３）　前記処理内容定義データが、可搬性を有する記録媒体に記録されたものであり、前記データ取込み部が、前記車両に搭載されたデータ読取り装置であって前記記録媒体が装填されてその記録媒体から前記処理内容定義データを読み取るものを含む（１）項に記載の車両基本機能制御プログラム更新装置［請求項３］。この装置においては、車両基本機能制御プログラムの更新が、オンラインではなく、記録媒体という物を使用することにより、行われる。したがって、この装置によれば、オンラインでの更新に固有の不都合、例えば、データ漏洩、不正アクセス等に対する配慮をそれほどせずに済み、車両基本機能制御プログラムの真正性を容易に維持し得る。

（４）　前記処理内容定義データが、前記処理の内容が暗号化された暗号データであり、前記プログラム更新部が、その暗号データが入力された場合に、その入力された暗号データを復号化する復号化部を含む（１）ないし（３）項のいずれかに記載の車両基本機能制御プログラム更新装置［請求項４］。この装置によれば、暗号デー

タの復号化によって車両基本機能制御プログラムが更新されるため、暗号データを使用せずにその更新を行う場合に比較し、車両基本機能制御プログラムが不正に更新されてしまう可能性が低減される。

（５）　さらに、前記車両が、前記取り込まれた処理内容定義データにより定義される処理が前記プログラムメモリに対して実行されることが予定された車両である予定プログラム更新対象車両ではない場合に、前記プログラム更新部による更新を禁止する第１更新禁止部を含む（１）ないし（４）項のいずれかに記載の車両基本機能制御プログラム更新装置［請求項５］。この装置においては、車両が、データ取込み部に取り込まれた処理内容定義データにより定義される処理がプログラムメモリに対して実行されることが予定された車両である予定プログラム更新対象車両ではない場合に、車両基本機能制御プログラムの更新が禁止される。したがって、この装置によれば、処理内容定義データと車両との実際の組み合わせが、その車両のメーカやディーラが予定した組み合わせと一致しない場合に、車両基本機能制御プログラムが予定外に更新されてしまうことが回避される。よって、この装置によれば、予定外の更新によって車両の基本機能が損なわれてしまうことを回避し得る。

（６）　前記第１更新禁止部が、前記処理内容定義データを識別するデータ識別情報と、前記車両を識別する車両識別情報とを外部にオンラインで送信することに応答してその外部からオンラインで受信した受信情報に基づき、前記車両が前記予定プログラム更新対象車両であるか否かを判定する判定手段と、その判定手段により前記車両が前記予定プログラム更新対象車両ではないと判定された場合に、前記プログラム更新部による更新を禁止する更新禁止手段とを含む（５）項に記載の車両基本機能制御プログラム更新装置。

（７）　さらに、前記車両の実際のユーザがその車両の真の所有者でもその真の所有者により許可された者でもない場合に、前記プログラム更新部による更新を禁止する第２更新禁止部を含む（１）ないし（６）項のいずれかに記載の車両基本機能制御プログラム更新装置［請求項６］。この装置においては、車両の実際のユーザがその車両の真の所有者でもその真の所有者により許可された者でもない場合に、車両基本機能制御プログラムの更新が禁止される。したがって、この装置によれば、車両の真の所有者の意に反して車両基本機能制御プログラムが更新されてしまうことを容易に回避し得る。

（８）　前記第２更新禁止部が、前記車両に実際に装着されたキーに搭載された発信回路から受信した受信信号に基づき、その実際のキーが真正であるか否かを判定する判定手段と、その判定手段によりその実際のキーが真正ではないと判定された場合に、前記プログラム更新部による更新を禁止する更新禁止手段とを含む（７）項に記載の車両基本機能制御プログラム更新装置。

（９）　前記プログラム更新部が、それが更新すべき前記車両基本機能制御プログラムを実行する前記コンピュータと同じコンピュータにより作動させられるものである（１）ないし（８）項のいずれかに記載の車両基本機能制御プログラム更新装置［請求項７］。この装置においては、車両基本機能制御プログラムの更新が、そのプログラムを実行するコンピュータと同じコンピュータにより行われる。したがって、この装置によれば、専用のコンピュータを追加せずに車両基本機能制御プログラムの更新が可能となる。よって、この装置によれば、車両基本機能制御プログラムの更新を経済的にも構造的にも有利に実施可能となる。

（１０）　さらに、前記コンピュータの負荷状態が設定状態を超えている場合に、前記プログラム更新部による更新を禁止する第３更新禁止部を含む（９）項に記載の車両基本機能制御プログラム更新装置［請求項８］。この装置においては、車両基本機能制御プログラムを実行すべきコンピュータの負荷状態が設定状態を超えている場合に、車両基本機能制御プログラムの更新が禁止される。したがって、この装置によれば、車両基本機能制御プログラムを実行すべきコンピュータの通常機能を犠牲にすることなく、そのコンピュータにより車両基本機能制御プログラムの更新を行い得る。

（１１）　前記第３更新禁止部が、前記車両が実質的に停止状態にはない場合に、前記コンピュータの負荷状態が設定状態を超えている場合であるとして、前記プログラム更新部による更新を禁止する更新禁止手段を含む（１０）項に記載の車両基本機能制御プログラム更新装置［請求項９］。車両が実質的に停止状態にはない場合には、実質的に停止状態にある場合に比較し、車両基本機能制御プログラムを実行すべきコンピュータがそのプログラムを実行するために占有される時間が長いと考えられる。このような知見に基づき、本項に係る装置においては、車両が実質的に停止状態にはない場合に、コンピュータの負荷状態が設定状態を超えている場合であるとして、そのコンピュータによる車両基本機能制御プログラムの更新が禁止される。したがって、この装置によれば、車両基本機能制御プログラムの更新を行うことが原因で、本来の動作、すなわち、車両基本機能制御プログラムの実行に支障を来たすことを容易に回避し得る。

（１２）　さらに、前記車両が実質的に停止状態にはない場合に、前記プログラム更新部による更新を禁止する第４更新禁止部を含む（１）ないし（１１）項のいずれかに記載の車両基本機能制御プログラム更新装置［請求項１０］。従来においては、前述の説明から明らかなように、車両の停止状態においてコンピュータを全体的にまたは部分的に交換することにより、車両基本機能制御プログラムの変更が行われていた。このように、従来においては、車両基本機能制御プログラムの変更が車両の停止状態で、すなわち、その車両のユーザにとって安全

な状態で行われていたのである。一方、これに倣い、前記（１）ないし（１１）項のいずれかに記載の車両基本機能制御プログラム更新装置を実施する際には、車両基本機能制御プログラムの更新を車両の実質的な停止状態で行うことが望ましいという考え方があり得る。そこで、本項に係る装置においては、車両が実質的に停止状態にはない場合に、車両基本機能制御プログラムの更新が禁止される。したがって、この装置によれば、車両基本機能制御プログラムの更新を、従来におけるとほぼ同じ状況で安全に行い得る。

（１３）　前記第４更新禁止部が、前記車両の状態を検出する車両状態センサと、その車両状態センサの出力信号に基づき、前記車両が実質的に停止状態にあるか否かを判定する判定手段と、その判定手段により前記車両が実質的に停止状態にはないと判定された場合に、前記プログラム更新部による更新を禁止する更新禁止手段とを含む（１２）項に記載の車両基本機能制御プログラム更新装置。

【００１１】

【発明の実施の形態】以下、本発明のさらに具体的な一実施形態を図面に基づいて詳細に説明する。

【００１２】図１には、本実施形態である車両基本機能制御プログラム更新装置（以下、単に「更新装置」という）の構成が機能ブロック図により概念的に表されている。この更新装置は、車両において基本機能制御プログラムを部品交換なしでオンラインで更新する装置であり、自動車等の車両に搭載される。

【００１３】この車両は、よく知られているように、エンジン（内燃機関）と電動機との少なくとも一方である駆動源からの動力により、複数の車輪のうちの少なくともいくつかである駆動車輪が駆動されることにより、駆動（走行）させられる。

【００１４】この車両は、それの状態が電子制御ユニット１０（以下、「ＥＣＵ」と略称する）により制御され、これにより、車両の基本機能である「走る」、「曲がる」および「止まる」といった動作が電子制御される。

【００１５】車両においてＥＣＵ１０により実行される制御の種類は、例えば、パワートレイン制御と、ボデー制御と、車両制御とに分類することができる。パワートレイン制御は、駆動源の制御と、駆動源の動力を駆動車輪に伝達する駆動系（トランスミッション、デファレンシャル等を含む）の制御とを含んでいる。ボデー制御は、エアバッグ等の乗員保護装置の制御を含んでいる。車両制御は、ブレーキ制御と、サスペンション制御と、ステアリング制御と、定速走行制御とを含んでいる。ブレーキ制御の一例は、車両制動時に各車輪のロック傾向が過大になることを防止するアンチロック制御である。

【００１６】この車両は、さらに、図２に示すように、ナビゲーション装置２０を備えている。ナビゲーション装置２０は、よく知られているように、運転者に対して車両の現在位置や目的地への経路を表示装置の地図上に表示する装置である。このナビゲーション装置２０は、ＦＭ多重文字放送や、道路上に設置されているビーコン（情報通信施設）を利用することにより、外部から電波によりデータを受信可能となっている。さらに、このナビゲーション装置２０は、携帯電話機およびＰＨＳを含む移動電話機２２が接続可能とされている。その接続により、この車両から外部へ電波によりデータを送信可能となる。

【００１７】このナビゲーション装置２０は、ＥＣＵ１０に接続されている。したがって、この車両においては、図１に示すように、外部としての車両ディーラ用サーバ３０（サーバ・コンピュータの一例である）および車両メーカ用サーバ３２（サーバ・コンピュータの一例である）からの送信データがナビゲーション装置２０を介してＥＣＵ１０により電波として受信可能であるとともに、そのＥＣＵ１０からの送信データがナビゲーション装置２０および移動電話機２２を介して外部へ電波で送信可能となっている。ここに、車両ディーラは、当該車両を正規に販売したり、修理したりする事業体である。また、車両メーカは、当該車両を正規に製造した事業体である。

【００１８】この車両は、図２に示すように、さらに、オーディオ装置４０を備えている。オーディオ装置４０は、よく知られているように、車内で音楽や放送等のオーディオソースをラジオ、カセットプレイヤ、ＣＤプレイヤ等によって聞くための装置である。このオーディオ装置４０には、ＣＤオートチェンジャ４２が接続されており、一度に装填された複数枚のＣＤが適宜選択されて再生される。このオーディオ装置４０もＥＣＵ１０に接続されており、これにより、ＥＣＵ１０は、それらオーディオ装置４０およびＣＤオートチェンジャ４２により、ＣＤからデータを有線で、すなわち、車内の情報通信ネットワーク５０を介して、受信可能となっている。

【００１９】ＥＣＵ１０は、よく知られているように、図３に示すように、ＣＰＵ６０とＲＯＭ６２とＲＡＭ６４とがバス６６により互いに接続されて構成されたコンピュータ７０を主体として構成されている。ＲＯＭ６２は、フラッシュメモリ８０をフラッシュＥＰＲＯＭとして含むように構成されている。図４に示すように、このフラッシュメモリ８０に、ＣＰＵ６０により実行されて車両の基本機能を制御する車両基本機能制御プログラムとして、例えば、駆動源制御プログラム、駆動系制御プログラムおよび車両制御プログラムが書換可能に記憶される。

【００２０】本実施形態においては、図１に示すように、ＥＣＵ１０が、さらに、復号化回路９０と書換回路９２とを含むように構成されている。

【００２１】復号化回路９０は、現在の車両基本機能制

御プログラムが書き換えられるべき内容を有する新規な車両基本機能制御プログラムであって関係者から入手したものを暗号で表す暗号データを復号化して復号データを作成するための回路である。復号化回路９０は、真正な復号鍵信号が入力されることに応答して、それに入力された暗号データを復号する。

【００２２】これに対して、書換回路９２は、その復号化回路９０により作成されて入力された復号データにより、フラッシュメモリ８０の内容を書き換えるための回路である。書換回路９２は、書換許可信号が入力されるのに応答して、上記入力された復号データにより、現在の車両基本機能制御プログラムの内容をフラッシュメモリ８０において書き換える。

【００２３】図１に示すように、ＥＣＵ１０のうちコンピュータ７０により構成される部分により、データ取込み部１００、認証部１０２、復号鍵信号送信部１０４および書換許可部１０６が構成されている。

【００２４】概略的に説明すれば、データ取込み部１００は、上述の暗号データを外部から取り込む部分である。認証部１０２は、外部から取り込まれた暗号データと、その車両との実際の組み合わせが真正であることを認証する部分である。復号鍵信号送信部１０４は、その認証部１０２による認証に応答し、後述のようにして外部から受信した復号鍵信号を上記復号化回路９０に供給する部分である。書換許可部１０６は、車両が実質的に停止状態にある場合に、書換許可信号を上記書換回路９２に供給する部分である。

【００２５】この書換許可部１０６は、車両が実質的に停止状態にあるか否かを判定するために、車両の状態を検出する車両状態センサに接続されている。その車両状態センサ１１０は、車体速度を検出する車体速度センサ（車輪の回転速度を検出する車輪速度センサで代用可）、駆動源の回転数を検出する回転数センサ、駆動系の状態を変更するために運転者により操作されるシフト操作部材としてのシフトレバーの操作位置を検出するシフト位置センサ等を含んでいる。

【００２６】本実施形態においては、その車両状態センサ１１０が、ＥＣＵ１０による車両基本機能制御にも使用されるようになっており、車両基本機能制御プログラムの更新に専用のものとはされていない。したがって、本実施形態によれば、車両基本機能制御プログラムのオンライン更新機能を車両に付加するのに伴うコストアップを容易に節減させ得る。

【００２７】それらデータ取込み部１００、認証部１０２、復号鍵信号送信部１０４および書換許可部１０６の各機能は、図５にフローチャートで概念的に表されている書換プログラムであってＲＯＭ６２の書換プログラムメモリ１１２（図３参照）に記憶されているものがＣＰＵ６０により実行されることにより、実現される。

【００２８】この書換プログラムは、繰り返し実行される。各回の実行時には、まず、ステップＳ１（以下、単に「Ｓ１」で表す。他のステップについても同じとする）において、図１に示す車両ディーラ用サーバ３０から、現在の車両基本機能制御プログラムが部分的に書き換えられるべき内容を有する新規の車両基本機能制御プログラムを表す暗号データを電波により受信したか否かが判定される。受信しなかった場合には、その判定がＮＯとなり、直ちにこの書換プログラムの一回の実行が終了する。

【００２９】これに対して、暗号データを受信した場合には、Ｓ１の判定がＹＥＳとなり、Ｓ２に移行する。このＳ２においては、その受信した暗号データが暗号データメモリ１２０（図３参照）であってＲＡＭ６４に設けられたものに一時的にストアされる。

【００３０】その後、Ｓ３において、その受信した暗号データを識別するための固有情報であるデータＩＤが、その暗号データから抽出される。さらに、このステップにおいては、当該車両を識別するための固有情報（例えば、車体番号）を表すデータである車両ＩＤが、例えば、ＲＯＭ６２やナビゲーション装置２０のコンピュータのＲＯＭから読み出される。さらに、このステップにおいては、それらデータＩＤと車両ＩＤとが、車両メーカ用サーバ３２に電波により送信される。

【００３１】その車両メーカ用サーバ３２においては、受信したデータＩＤと車両ＩＤとの組み合わせが、予め登録してある複数の組み合わせの中に一致するものがあるか否かが判定される。認証の成否が判断されるのである。この判断は、車両が受信した暗号データによってその車両の車両基本機能制御プログラムを書き換えることが車両ディーラまたは車両メーカが意図したことであるか否かが判定されるのである。

【００３２】認証が成立した場合には、車両メーカ用サーバ３２は、そのことを表す認証情報を電波によりその車両に送信する。その認証情報を受信した車両においては、Ｓ４の判定がＹＥＳとなり、Ｓ５に移行する。

【００３３】これに対して、車両メーカ用サーバ３２から認証情報を受信しない状態が設定時間以上継続した場合には、Ｓ４ａの判定がＹＥＳとなり、今回は、受信した暗号データによる車両基本機能制御プログラムの書換が不適当であるとして、Ｓ１０において、書換不許可信号が書換回路９２に送信される。以上で、この書換プログラムの今回の実行が終了する。したがって、本実施形態においては、データＩＤと車両ＩＤとの実際の組み合わせが真正ではない場合には、車両基本機能制御プログラムの書換が禁止される。

【００３４】Ｓ５においては、当該車両において現在使用されているキー１２２（図１参照）から復号鍵信号を受信したか否かが判定される。ここに、キー１２２は、よく知られているように、車両電源の投入・切断および駆動源の起動・停止を指令するために運転者により、車

両の所定位置に差し込まれて操作される物理的存在である。本実施形態においては、実際のキー１２２が真正である場合には、そのキー１２２に装着された発信回路１２４（図１参照）が、真正の復号鍵信号を車両の受信回路（車両のうち、キー１２２が差し込まれる位置に近接して配置されている。図示しない）に向けて発するようになっている。

【００３５】復号鍵信号が真正であるか否かを問わず、復号鍵信号をキー１２２から上記受信回路を経てＥＣＵ１０が受信した場合には、図５のＳ５の判定がＹＥＳとなり、Ｓ６に移行する。

【００３６】これに対して、キー１２２から復号鍵信号を受信しない状態が設定時間以上継続した場合には、Ｓ５ａの判定がＹＥＳとなる。この場合、現に使用されているキー１２２が真正でないため、受信した暗号データによる車両基本機能制御プログラムの書換が不適当であるとして、Ｓ１０において、書換不許可信号が書換回路９２に送信される。以上で、この書換プログラムの今回の実行が終了する。

【００３７】Ｓ６においては、その受信した復号鍵信号が復号化回路９０に送信される。その送信に応答し、復号化回路９０は、その復号鍵信号が真正である場合には、暗号データメモリ１２０から暗号データを取り込んで復号化を行い、復号データを書換回路９２に出力する。しかし、復号化回路９０は、その復号鍵信号が真正ではない場合には、暗号データメモリ１２０から暗号データを取り込むことも復号化も行わず、復号データを書換回路９２に出力することもしない。したがって、本実施形態においては、キー１２２から受信した復号鍵信号が真正ではない場合には、車両基本機能制御プログラムの書換が禁止される。

【００３８】その後、Ｓ７において、車両状態センサ１１０から、現在の車両状態を表す車両状態信号が入力される。続いて、Ｓ８において、その入力された車両状態信号に基づき、車両が実質的に停止状態にあるか否かが判定される。具体的には、前記車体速度センサからの信号が車体速度が０に十分に近い設定速度以下であることを表しているという条件と、前記回転数センサからの信号が駆動源の回転数が０に十分に近い設定回転数以下であることを表しているという条件と、前記シフト位置センサからの信号がシフトレバーがパーキング操作位置にあることを表しているという条件とが互いに一緒に成立したか否かが判定され、成立した場合には、車両が実質的に停止状態にあると判定され、一方、成立しない場合には、車両が実質的に停止状態にはないと判定される。車両が実質的に停止状態にあれば、ＥＣＵ１０のコンピュータ７０の負荷がかなり小さく、車両基本機能制御プログラムの書換を行わせても、そのコンピュータ７０に支障を来すおそれはほとんどないと予想される。

【００３９】今回は、車両が実質的に停止状態にあると仮定すれば、Ｓ８の判定がＹＥＳとなり、Ｓ９に移行するが、今回は、車両が実質的に停止状態にはないと仮定すれば、Ｓ８の判定がＮＯとなる。その後、Ｓ８ａにおいて、Ｓ８の判定がＮＯである状態が設定時間以上継続したか否かが判定される。継続していない場合には、判定がＮＯとなり、Ｓ７に戻るが、継続した場合には、判定がＹＥＳとなり、Ｓ１０において、書換不許可信号が書換回路９２に送信される。この場合、車両基本機能制御プログラムの書換が禁止される。以上で、この書換プログラムの今回の実行が終了する。

【００４０】Ｓ９においては、書換許可信号が書換回路９２に送信される。その送信に応答し、書換回路９２は、復号化回路９０から復号データが出力されることを条件に、その復号データで現在の車両基本機能制御プログラムを部分的に書き換える。したがって、キー１２２から受信した復号鍵信号が真正ではない場合には、たとえ車両メーカ用サーバ３２から認証情報を受信し、かつ、車両が実質的に停止状態にある場合であっても、暗号データによる車両基本機能制御プログラムの書換が禁止される。

【００４１】以上で、この書換プログラムの一回の実行が終了する。

【００４２】以上の説明から明らかなように、本実施形態においては、ＥＣＵ１０のうち図５のＳ２を実行する部分がデータ取込み部１００を構成し、Ｓ３およびＳ４を実行する部分が認証部１０２を構成し、Ｓ５およびＳ６を実行する部分が復号鍵信号送信部１０４を構成し、Ｓ７ないしＳ９を実行する部分が書換許可部１０６を構成しているのである。

【００４３】以上の説明から明らかなように、本実施形態においては、ＥＣＵ１０のコンピュータ７０が請求項１における「コンピュータ」の一例を構成し、フラッシュメモリ８０が同請求項における「プログラムメモリ」の一例を構成し、暗号データが同請求項における「処理内容定義データ」の一例を構成し、少なくともデータ取込み部１００が同請求項における「データ取込み部」の一例を構成し、少なくともＥＣＵ１０のコンピュータ７０のうち図５の書換プログラムを実行する部分と、復号化回路９０と、書換回路９２とが互いに共同して同請求項における「プログラム更新部」の一例を構成しているのである。

【００４４】さらに、本実施形態においては、ナビゲーション装置２０とデータ取込み部１００とが互いに共同して請求項２における「データ受信部」の一例を構成しているのである。

【００４５】さらに、本実施形態においては、復号化回路９０が請求項４における「復号化部」の一例を構成しているのである。

【００４６】さらに、本実施形態においては、認証部１０２と復号化回路９０のうち復号化を真正の復号鍵信号

の受信時に限って許可する部分とが互いに共同して請求項５における「第１更新禁止部」の一例を構成しているのである。

【００４７】さらに、本実施形態においては、発信回路１２４と復号鍵信号送信部１０４と復号化回路９０のうち復号化を真正の復号鍵信号の受信時に限って許可する部分とが互いに共同して請求項６における「第２更新禁止部」の一例を構成しているのである。

【００４８】さらに、本実施形態においては、少なくともＥＣＵ１０のコンピュータ７０のうち図５の書換プログラムを実行する部分と、復号化回路９０と、書換回路９２とが互いに共同して請求項７における「プログラム更新部」の一例を構成し、車両基本機能制御プログラムの実行と更新とが同じコンピュータ７０により実施されるようになっているのである。

【００４９】さらに、本実施形態においては、車両状態センサ１１０と書換許可部１０６と書換回路９２のうち書換を書換許可信号の受信時に限って許可する部分とが互いに共同して請求項８における「第３更新禁止部」の一例、および請求項９における「更新禁止手段」の一例を構成しているのである。

【００５０】さらに、本実施形態においては、車両状態センサ１１０と書換許可部１０６と書換回路９２のうち書換を書換許可信号の受信時に限って許可する部分とが互いに共同して請求項１０における「第４更新禁止部」の一例を構成しているのである。

【００５１】なお付言すれば、本実施形態においては、暗号データが、車両ディーラ用サーバ３０から送信される電波により搬送されてＥＣＵ１０に取り込まれるようになっているが、このような態様で暗号データをＥＣＵ１０が取り込むことは本発明を実施する上において不可欠なことではない。例えば、暗号データをＣＤ（コンパクトディスク）に記録するとともに、ＥＣＵ１０に接続されたオーディオ装置４０およびＣＤオートチェンジャ４２をデータ読取り部として機能させることにより、そのＣＤオートチェンジャ４２にそのＣＤを装填してそのＣＤから必要なデータを読み取らせることにより、暗号データをＥＣＵ１０に取り込むようにして本発明を実施することが可能なのである。

【００５２】さらに付言すれば、本実施形態においては、フラッシュメモリ８０における車両基本機能制御プログラムの更新の選択的禁止が、復号化過程と書換過程との双方において行われるようになっている。復号化回路９０と書換回路９２との双方を利用することにより行われるようになっているのであるが、このような態様で更新の選択的禁止を実行することは本発明を実施する上において不可欠なことではない。例えば、それら復号化過程と書換過程とのいずれかのみにおいて更新の選択的禁止が行われるようにして本発明を実施することが可能なのである。

【００５３】さらに付言すれば、本実施形態においては、フラッシュメモリ８０における車両基本機能制御プログラムの更新が、データＩＤと車両ＩＤとの組み合わせに関する認証と、車両のキー１２２に関する認証との双方が一緒に成立しない限り、禁止されるようになっているが、このような態様で更新の選択的禁止を実行することは本発明を実施する上において不可欠なことではない。例えば、フラッシュメモリ８０における車両基本機能制御プログラムの更新が、データＩＤと車両ＩＤとの組み合わせに関する認証と、車両のキー１２２に関する認証とのいずれかが成立しない限り、禁止されるようにして本発明を実施することが可能なのである。

【００５４】さらに付言すれば、本実施形態においては、プログラム更新部がＥＣＵ１０のコンピュータ７０のうち書換プログラムを実行する部分と、復号化回路９０および書換回路９２という専用の電子回路との組み合わせにより構成されるようになっているが、このような態様でプログラム更新部を構成することは本発明を実施する上において不可欠なことではない。例えば、ＥＣＵ１０のコンピュータ７０または専用のコンピュータにより、上記書換プログラムと同じプログラムの他、復号化回路９０に代わる復号化プログラムと、書換回路９２に代わる復号データ書換プログラムとを実行させることにより、それらコンピュータ７０または専用コンピュータの一部としてプログラム更新部が構成されるようにして本発明を実施することが可能なのである。

【００５５】さらに付言すれば、本実施形態においては、更新されるべき車両基本機能制御プログラムがフラッシュメモリ８０としてのフラッシュＥＰＲＯＭに記憶されるようになっているが、このような態様で車両基本機能制御プログラムメモリを構成することは本発明を実施する上において不可欠なことではない。例えば、ＦＰＧＡ(Field Programmable Gate Array)を用いて車両基本機能制御回路とプログラムメモリとが構成されるようにして本発明を実施することが可能なのである。この態様によれば、例えば、車両基本機能制御プログラムの更新に必要な時間を容易に短縮し得る。

【００５６】以上、本発明の一実施形態を図面に基づいて詳細に説明したが、これは例示であり、前記［課題を解決するための手段および発明の効果］の欄に記載の態様を始めとして、当業者の知識に基づいて種々の変形、改良を施した他の形態で本発明を実施することが可能である。

【図面の簡単な説明】

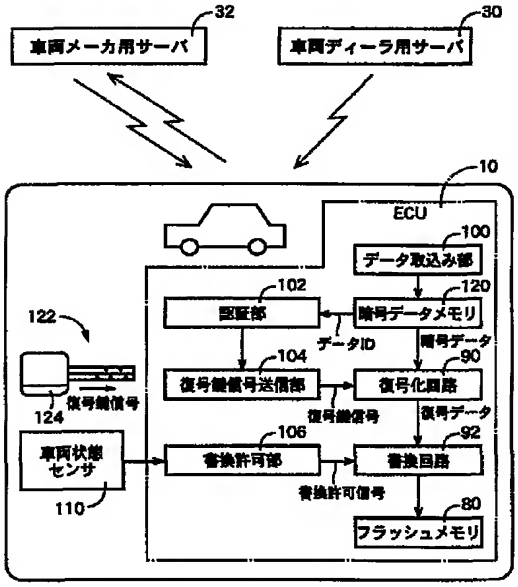
【図１】本発明の一実施形態である車両基本機能制御プログラム更新装置の構成を概念的に表す機能ブロック図である。

【図２】図１における車両の内部における情報通信ネットワーク５０を説明するための図である。

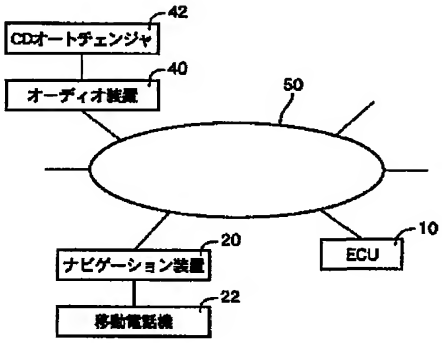
【図３】図１におけるＥＣＵ１０の構成を概念的に表す

ブロック図である。
【図４】図３におけるフラッシュメモリ８０の構成を概念的に表すブロック図である。
【図５】図３におけるＥＣＵ１０により実行される書換プログラムの内容を概念的に表すフローチャートである。
【符号の説明】
１０　電子制御ユニットＥＣＵ
２０　ナビゲーション装置
３０　車両ディーラ用サーバ
３２　車両メーカ用サーバ
４０　オーディオ装置
４２　ＣＤオートチェンジャ
＊７０　コンピュータ
８０　フラッシュメモリ
９０　復号化回路
９２　書換回路
１００　データ取込み部
１０２　認証部
１０４　復号鍵信号送信部
１０６　書換許可部
１１０　車両状態センサ
１２０　暗号データメモリ
１２２　キー
１２４　発信回路
＊

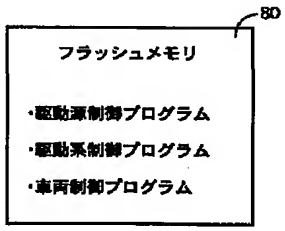
【図１】



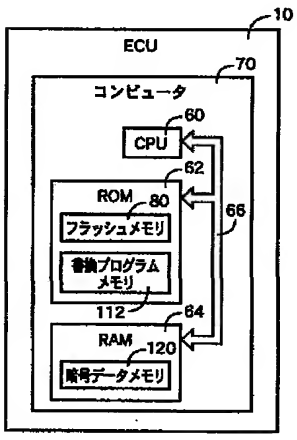
【図２】



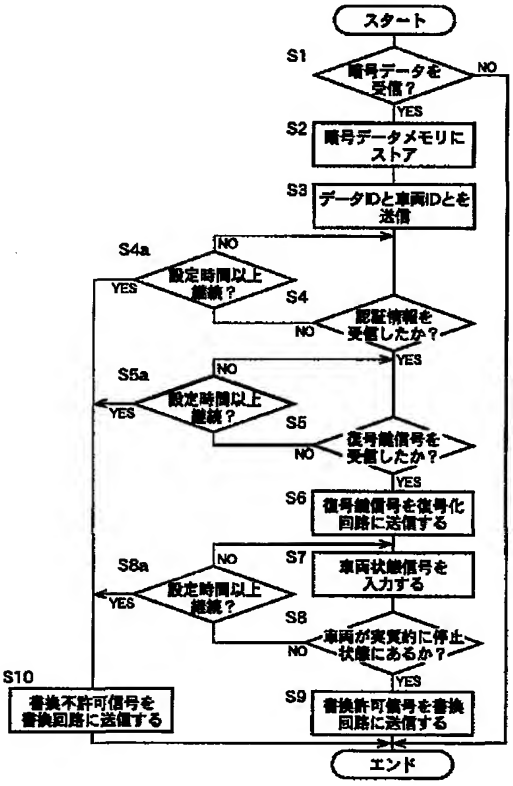
【図４】



【図３】



【図５】



フロントページの続き

(72)発明者　加藤　覚
愛知県愛知郡長久手町大字長湫字横道41番地の１　株式会社豊田中央研究所内
(72)発明者　前田　光俊
愛知県愛知郡長久手町大字長湫字横道41番地の１　株式会社豊田中央研究所内
(72)発明者　米村　正寿
愛知県愛知郡長久手町大字長湫字横道41番地の１　株式会社豊田中央研究所内
(72)発明者　伊藤　博
愛知県愛知郡長久手町大字長湫字横道41番地の１　株式会社豊田中央研究所内

Ｆターム(参考)　5B076 EA18 EB01 FA00
5H215 AA10 BB10 CC09 CX01 GG04 KK07